

Sep 27, 2023

s/ JDH

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))

Information associated with Facebook User ID)

100087649156218, which is stored at premises owned,
maintained, controlled, or operated by Meta Platforms, Inc., as
further described in Attachment A)

Case No. 23-M-472 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 10-11-23 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: 9-27-23. 1:40 pm

Stephen C. Dries

Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Facebook User ID 100087649156218 for the time period of April 1, 2023, through the date of this warrant, which is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A **for the time period of April 1, 2023, through the date of this warrant.**

- (a) All contact and personal identifying information for Target Account including, full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the accounts and all other documents showing the user’s posts and other Facebook activities.
- (c) All photos and videos uploaded by those user IDs and all photos and videos uploaded by any user that have those users tagged in them including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos.
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which

the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string.
- (f) All other records and contents of communications and messages made or received by the user including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests.
- (g) All "check ins" and other location information.
- (h) All IP logs, including all records of the IP addresses that logged into the account.
- (i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked".
- (j) All information about the Facebook pages that the accounts were or are a "fan" of.
- (k) All past and present lists of friends created by the accounts.
- (l) All records of Facebook searches performed by the accounts.
- (m) All information about the user's access and use of Facebook Marketplace.
- (n) The types of service utilized by the user.

- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number).
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account.
- (q) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

The Target Provider shall disclose responsive data, if any, within **fourteen days (14)** of the **ISSUANCE** of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1951 (Hobbs Act robbery) and 924(c) (brandishing a firearm during a crime of violence) Jamal White or others, including, information pertaining to the following matters:

1. Images or descriptions of clothing, accessories, vehicles, or weapons potentially used in robberies;
2. Information or communications concerning robberies, or potential robbery targets, or rewards for the disclosure of information regarding completed robberies;
3. Communications reflecting connections between robbery suspects and their relatives;
4. Information or communications concerning robbery proceeds or cash windfalls;

5. Financial records, including account information, bank statements, checks, money orders, cash, ATMs, withdrawals, deposits, transfers (including wire, ACH transfers);
6. All evidence of who created, used, owned, or controlled the Target Account, including, records that help reveal the identity and whereabouts of such person(s);
7. Evidence indicating how and when the Target Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the Target Account owner;
8. Evidence indicating the Target Account owner's state of mind as it relates to the crimes under investigation; and
9. The identity of the person(s) who communicated with the Target Accounts about matters relating to the above-mentioned violations, including records that help reveal their whereabouts.

Sep 27, 2023

s/ JDH

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Information associated with Facebook User ID 100087649156218,
which is stored at premises owned, maintained, controlled, or operated
by Meta Platforms, Inc., as further described in Attachment A

Case No. 23-M-472 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 1951 and 924(c)	Hobbs Act robbery, and brandishing a firearm during a crime of violence.

The application is based on these facts:
See Attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



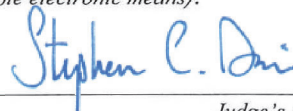
Applicant's signature

Kevin Kaiser, FBI SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ *(specify reliable electronic means)*.

Date: 9-27-23



Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Kevin Kaiser, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), a company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

2. **Your Affiant.** I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since April 2023. Since April 2023, I have been assigned to FBI’s Milwaukee Area Violent Crimes Task Force (MAVCTF), a multi-jurisdictional law enforcement entity charged with investigating violations of federal law, including bank robberies, commercial robberies, armed motor vehicle robberies, and other violent crime matters, defined under Title 18 of the United States Code. I have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have participated in criminal investigations, surveillance, search warrants, interviews, and debriefs of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

3. I make this affidavit in support of an application for a search warrant for information associated with Facebook User ID 100087649156218 (the “Target Account”). Information pertaining to this account is stored at premises owned, maintained, controlled, or operated by Meta Platforms (“Meta”), a social networking company headquartered at 1601 Willow Road, Menlo Park, California, 94025 (the “Target Provider”), further described herein and in Attachment A respectively (attached hereto and incorporated herein).

4. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Target Provider to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber and customer associated with the Target Account, further described in Section I of Attachment B (attached hereto and incorporated herein). Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate and seize the items described in Section II of Attachment B.

5. Based on the investigation to date, I submit that there is probable cause to believe that Jamal M. White (DOB XX/XX/1990) committed seven armed robberies throughout the Eastern District of Wisconsin and Northern District of Illinois on May 19, 2023 and May 21, 2023, in violation of Title 18, United States Code, Sections 1951(a) (Hobbs Act robbery), and 924(c) (brandishing a firearm during a crime of violence).

6. **Sources of Information.** The facts in this affidavit come from my personal observations, my training and experience, information obtained from other agents and witnesses, public records, and my own investigative efforts. I believe these sources of information to be credible and reliable based on the corroboration of the information and my experience with these

matters. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

7. **Jurisdiction.** This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

II. PROBABLE CAUSE

Robbery 1 – Speedway, West Allis – 5/19/23

8. On 05/19/2023 at approximately 1:16 pm, a black male wearing a black mask entered and conducted an armed robbery of the Speedway gas station located at 9111 W. National Avenue, West Allis, in the County of Milwaukee, and the State and Eastern District of Wisconsin. The suspect (Suspect 1) approached the counter and asked the cashier for Newport cigarettes. The cashier observed Suspect 1 retrieve a gun from what she believed was his front sweatshirt pocket. Suspect 1 pointed the gun directly at the cashier and told her to give him all the money. Suspect 1 obtained an estimated total of \$797.00 from the robbery and fled from the gas station.

9. Suspect 1 exited the gas station and traveled north on foot. Video surveillance obtained from a nearby business showed Suspect 1 run behind a silver vehicle and enter the front driver’s side of the vehicle. The silver vehicle then traveled southbound on South 90’th Street. The vehicle was later identified as a 2019 Nissan Versa bearing IL registration CF 47396.

10. Suspect 1 was described as a black male, approximately 5'08"-5'09" with a skinny build, wearing a black hooded sweatshirt with a tan or camouflage Timberland logo, blue jeans, black ski mask, black gloves, black shoes, carrying a black firearm.

Robbery 2 – BP, West Allis – 5/19/23

11. On 05/19/2023 at approximately 1:32 pm, a black male wearing a black mask entered and conducted an armed robbery of the BP gas station located at 2310 South 76th Street, West Allis, in the County of Milwaukee, and the State and Eastern District of Wisconsin. The subject (Suspect 1) approached the counter and asked the cashier for a pack of Newport cigarettes. As the cashier was handing the cigarettes to Suspect 1, Suspect 1 pulled a firearm from the pocket of his hooded sweatshirt and demanded money from the register. The cashier provided Suspect 1 with approximately \$300 after which Suspect 1 fled from the store eastbound on foot.

12. Suspect 1 was described as a black male, approximately 5'08"-5'09", wearing a light gray hooded sweatshirt with black graffiti-type writing, black jeans, and a black mask covering the lower half of his face. He had short dreadlocks hanging out of the hooded sweatshirt and displayed a black handgun.

Robbery 3 – Walgreens, Milwaukee – 5/19/23

13. On 05/19/2023 at approximately 1:44 pm, a black male wearing a black mask entered and conducted an armed robbery of the Walgreens located at 6030 West Oklahoma Avenue, Milwaukee, in the County of Milwaukee, and the State and Eastern District of Wisconsin. The subject (Suspect 1) approached a cash register and asked the cashier for a pack of Newport cigarettes. When the cashier provided the cigarettes, Suspect 1 displayed a firearm and demanded money from the register. The cashier handed Suspect 1 cash from the register at which time Suspect 1 turned to leave the store. Suspect 1 then turned toward a second cash register, displayed the same firearm, and demanded money from the second cashier. When the

second cashier provided Suspect 1 with money from the register, Suspect 1 fled the store on foot. Suspect 1 obtained approximately \$664 from the two cash registers.

14. Video surveillance obtained from nearby businesses and residences showed Suspect 1 flee in a silver sedan consistent with the Nissan Versa from Robbery 1.

15. Suspect 1 was described as a black male, approximately 5'08", thin build, medium to dark complexion, wearing a white long-sleeved shirt, blue jeans, black shoes, a black mask covering the lower half of his face, carrying a black handgun.

Robbery 4 – Speedway, Greenfield – 5/19/23

16. On 05/19/2023 at approximately 2:06 pm, a black male wearing a black mask entered and conducted an armed robbery of the Speedway gas station located at 4265 South 60th Street, Greenfield, in the County of Milwaukee, and the State and Eastern District of Wisconsin. The subject (Suspect 1) approached the counter and asked the cashier for a pack of Newport cigarettes. When the cashier requested identification, Suspect 1 pulled a firearm out of the pocket of his hooded sweatshirt and demanded money from the register. The cashier provided Suspect 1 with approximately \$319 at which time he fled from the store.

17. After reviewing surveillance video from the store, responding detectives observed a silver sedan consistent with a Nissan Versa drive past the robbery location approximately one minute after the robbery occurred.

18. Suspect 1 was described as a black male, thin build, wearing a black hooded sweatshirt with a gold symbol on front, a black facemask, carrying a black firearm. Of note, the black hooded sweatshirt was identical to the black hooded sweatshirt worn in Robbery 1 (Speedway, West Allis).

Robbery 5 – Kenosha – 5/21/23

19. On 05/21/2023 at approximately 2:19 am, two black males wearing black masks entered and conducted an armed robbery of the Kwik Trip gas station located at 8012 39th Avenue, Kenosha, in the County of Kenosha, and the State and Eastern District of Wisconsin. The subjects (Suspect 1 and Suspect 2) loitered near the front of the store after which Suspect 2 exited the store and Suspect 1 approached the cashier and asked for a pack of Newport cigarettes. As the cashier was retrieving the cigarettes, Suspect 1 presented a firearm and demanded money from the register. The cashier provided approximately \$4243 to Suspect 1 at which time he exited the store.

20. After reviewing surveillance videos from surrounding businesses and residences, it was determined that the suspects fled in a white Dodge Nitro. The vehicle was later identified as a 2007 Dodge Nitro bearing IL registration TTQ 605.

21. Suspect 1 was described as a black male with a thin build and medium complexion, wearing a gray hooded sweatshirt with black “hustle” writing, blue jeans, a black mask, black gloves, and red shoes. He was carrying a black firearm. Of note, the gray hooded sweatshirt was identical to the gray hooded sweatshirt worn in Robbery 2 (BP, West Allis)

22. Suspect 2 was described as a black male with a thin build and medium complexion, wearing a black Nike hooded sweatshirt, black pants with white stripes, a black mask, white gloves, and black shoes with white soles.

Other Acts Committed

23. On May 21, 2023 at approximately 3:19 AM, two black males wearing black masks entered and committed an armed robbery of the Walgreens located at 1811 Belvidere Rd., Waukegan, Illinois. The subjects (Suspect 1 and Suspect 2) approached the cash register at which point Suspect 1 and Suspect 2 presented firearms and demanded money from the register.

Suspect 1 took approximately \$10-20 from a customer who was standing near the register after which he took approximately \$3,000 from the register tray and handed it to Suspect 2. The suspects then fled on foot from the store.

24. Suspect 1 was described as a black male with a thin build, wearing a white hooded sweatshirt with black writing, blue jeans, black gloves, black mask, and red shoes with white soles.

25. Suspect 2 was described as a black male with a thin build, wearing a black hooded sweatshirt, black pants with white stripes down the side, white gloves, black mask, and black shoes with white soles.

26. On May 21, 2023 at approximately 5:00 AM, two black males wearing black masks entered the Walgreens located at 4343 N Central Ave, Chicago, Illinois. The subjects (Suspect 1 and Suspect 2) approached the cash register where Suspect 1 requested a pack of gum. When the cashier opened the cash register, Suspect 1 presented a firearm and demanded money from the register. The cashier placed approximately \$700 in a plastic bag and handed it to Suspect 1 at which time both suspects fled from the store.

27. Suspect 1 was described as a black male wearing gray and white hooded sweatshirt, blue jeans, red shoes, and a black mask.

28. Suspect 2 was described as a black male wearing a black hooded sweatshirt, black pants, and a black mask.

T-Mobile True Call Data

29. On June 09, 2023, pursuant to a search warrant through the United States District Court for the Eastern District of Wisconsin, T-Mobile provided true call data for T-Mobile cellular towers in the area of robberies 1-5 along with the two additional Illinois robberies. T-

Mobile True Call data showed that the International Mobile Subscriber Identity (IMSI) 310240316316629 had records consistent with being in the area of robberies 1-5 at the time the robberies occurred.

30. On June 17, 2023, pursuant to a search warrant through the United States District Court for the Eastern District of Wisconsin, T-Mobile provided call detail records (CDR) and historical cell site data for IMSI 310240316316629. T-Mobile advised that IMSI 310240316316629 was associated with phone number 708-466-9775. T-Mobile provided CDRs and historical cell site data for phone number 708-466-9775, which showed records for that number being consistent with being in the area of robberies 1-5 along with the two additional Illinois robberies at the time the robberies occurred. T-Mobile advised that Dish Network LLC maintained all subscriber information for IMSI 310240316316629.

31. On June 27, 20223, Dish Network LLC provided subscriber information for phone number 708-466-9775. At the time the robberies occurred the listed subscriber was Jamal White.

AT&T Tower Dump

32. On June 12, 2023, pursuant to a court order through the United States District Court for the Eastern District of Wisconsin, AT&T provided tower dump information for AT&T cellular towers in the area of robberies 1-5 along with the two additional Illinois robberies. AT&T tower dump data showed that phone number 708-986-4159 had records consistent with being in the area of robberies 1-5 along with the two additional Illinois robberies at the time the robberies occurred.

33. On June 14, 2023, pursuant to a search warrant through the United States District Court for the Eastern District of Wisconsin, AT&T provided call detail records (CDR), historical

cell site data, and subscriber information for phone number 708-986-4159. At the time the robberies occurred the listed subscriber was Jamal White. Historical cell site data showed that the device had records consistent with being in the area of the robbery at the time the robbery occurred.

Illinois I-Pass

34. On June 06, 2023, Illinois I-Pass provided a photograph from the Illinois Tollway Plaza 21, southbound lane near Waukegan, Illinois. The photograph is of a violation of a Nissan Versa consistent with the suspect vehicle from robberies 1-4. The photograph was captured on May 29, 2023 at 2:35 PM.

35. A review of the T-Mobile historical cell site data from phone number ~~708-466-9775~~ showed that the device was consistent with being in the area of Illinois Tollway Plaza 21 at the time the violation photograph was captured.

36. The violation photograph depicts a black male driver with shoulder length dreadlocks, wearing a white shirt and actively using a cell phone. The suspect and suspect clothing are consistent with the suspect and suspect clothing from robbery 3 (Walgreens, Milwaukee).

Identification of Jamal White

37. After receiving subscriber information for the T-Mobile phone number and AT&T phone number, MAVCTF members located an Illinois Department of Corrections booking photograph for Jamal White, date of birth 07/10/1990. WHITE was on parole for a series of armed business robberies that occurred in 2015 and 2016. He was released in September 2022 after serving six years of a possible 15-year sentence. Further, WHITE was on bond for

five armed business robberies and one attempted armed business robbery that were charged on August 24, 2016 in Hammond, Indiana.

Arrest of Jamal White

38. On August 12, 2023 Calumet City police officers conducted a traffic stop of a silver Nissan Versa bearing Illinois registration CF47396. Jamal White was the driver and sole occupant of the Versa. White was taken into custody on an arrest warrant out of FBI Milwaukee for multiple Hobbs Act robberies. White had a BLU Products model G40 black cellphone on his person at the time of the arrest. White's phone was seized by Calumet City police officers and was sent to FBI Milwaukee Field Office. The cellphone is currently in evidence at the FBI Milwaukee Field Office.

39. Members of the FBI's MAVCTF coordinated with FBI Chicago surveillance teams and determined Jamal White was living at 1306 Sibley Blvd, Apt 2, Calumet City, IL. Ferrell Freeman, the registered owner of the Nissan Versa bearing Illinois registration CF47396, also lives at 1306 Sibley Blvd, Calumet City, IL. Surveillance teams observed White leave the 1306 Sibley Blvd address several times and return to the address later in the day. Surveillance teams also observed White drive the Nissan Versa on multiple occasions, while he was the sole occupant. On August 16, 2023, members of the MAVCTF obtained a signed search warrant from the Northern District of Illinois for 1306 Sibley Blvd, Apt 2, Calumet City, IL. On August 18, 2023, members of the MAVCTF coordinated with members of the FBI's Chicago Violent Crime Task Force to execute the search warrant at 1306 Sibley Blvd, Apt 2, Calumet City, IL. During the search, a black Glock 43X pistol (s/n BWUP623) was located in the apartment. The 43X matches the description of the gun used in the aforementioned robberies. The 43X was seized by members of the MAVCTF and transported to FBI Milwaukee for evidence processing.

40. The Facebook page “**Marco Kash**” (Facebook User ID 100087649156218) was located by members of FBI MAVCTF and contained images of Jamal White.

III. TECHNICAL INFORMATION REGARDING FACEBOOK¹

41. Meta owns and operates Facebook, a free-access social networking website that can be accessed at <http://www.facebook.com>. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

42. Meta asks Facebook users to provide basic contact and personal identifying information either during the registration process or thereafter. This information may include the user’s full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

43. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account

¹ The information in this section is based on information published by Meta on its Facebook website, including, but not limited to, the following webpages: “Privacy Policy,” available at <https://www.facebook.com/privacy/policy>; “Terms of Service,” available at <https://www.facebook.com/legal/terms>; “Help Center,” available at <https://www.facebook.com/help>; and “Information for Law Enforcement Authorities,” available at <https://www.facebook.com/safety/groups/law/guidelines/>.

includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

44. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

45. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

46. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can "tag" other users in a photo or video and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

47. Facebook users can use Facebook Messenger to communicate with other users via text, voice, video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

48. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

49. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

50. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

51. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

52. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

53. In addition to the applications described above, Meta provides users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that

application may appear on the user's profile page.

54. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user's IP address is retained by Meta along with a timestamp.

55. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables "Location History," "checks-in" to an event, or tags a post with a location.

56. Social networking providers like Meta typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

57. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Meta, can

indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

58. Therefore, the servers of Meta are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

NEXUS:

59. Based upon Facebook's capabilities as described above, affiant believes the requested data is likely to contain evidence of these crimes such as: images of White wearing any of the clothing he wore during the robberies; connections to Suspect 2 (Chils Clemons) and/or the registered owner of the Nissan Versa and recovered firearm (Ferrell Freeman); communications with those individuals or unknown others about the robberies; and searches and location data relevant to the robbery locations.

IV. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

60. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

V. CONCLUSION

61. Based on the foregoing, I request that the Court issue the proposed search warrant.

62. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Facebook User ID 100087649156218 for the time period of April 1, 2023, through the date of this warrant, which is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A **for the time period of April 1, 2023, through the date of this warrant.**

- (a) All contact and personal identifying information for Target Account including, full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the accounts and all other documents showing the user’s posts and other Facebook activities.
- (c) All photos and videos uploaded by those user IDs and all photos and videos uploaded by any user that have those users tagged in them including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos.
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which

the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string.
- (f) All other records and contents of communications and messages made or received by the user including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests.
- (g) All "check ins" and other location information.
- (h) All IP logs, including all records of the IP addresses that logged into the account.
- (i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked".
- (j) All information about the Facebook pages that the accounts were or are a "fan" of.
- (k) All past and present lists of friends created by the accounts.
- (l) All records of Facebook searches performed by the accounts.
- (m) All information about the user's access and use of Facebook Marketplace.
- (n) The types of service utilized by the user.

- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number).
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account.
- (q) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

The Target Provider shall disclose responsive data, if any, within **fourteen days (14)** of the **ISSUANCE** of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1951 (Hobbs Act robbery) and 924(c) (brandishing a firearm during a crime of violence) Jamal White or others, including, information pertaining to the following matters:

1. Images or descriptions of clothing, accessories, vehicles, or weapons potentially used in robberies;
2. Information or communications concerning robberies, or potential robbery targets, or rewards for the disclosure of information regarding completed robberies;
3. Communications reflecting connections between robbery suspects and their relatives;
4. Information or communications concerning robbery proceeds or cash windfalls;

5. Financial records, including account information, bank statements, checks, money orders, cash, ATMs, withdrawals, deposits, transfers (including wire, ACH transfers);
6. All evidence of who created, used, owned, or controlled the Target Account, including, records that help reveal the identity and whereabouts of such person(s);
7. Evidence indicating how and when the Target Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the Target Account owner;
8. Evidence indicating the Target Account owner's state of mind as it relates to the crimes under investigation; and
9. The identity of the person(s) who communicated with the Target Accounts about matters relating to the above-mentioned violations, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Meta Platforms, Inc. (“Meta”), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Meta. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Meta, and they were made by Meta as a regular practice; and

b. such records were generated by Meta’s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Meta in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Meta, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature